Internet Safety

Managing your risks
Objectives

- Increase knowledge and awareness of internet risks
- Become familiar with lingo
- Learn how to keep computer ‘clean’
- Gain confidence that internet safety is manageable
Today’s Topics

• Malware
• Identity theft
• Account hacking
• Scams and frauds
• Cyberbullying
Strike a Balance

Digital Age Advantages

Risk Awareness
Risks are highly interconnected

Falling victim to one risk may make you more vulnerable to another...

But protecting yourself from each risk makes you less vulnerable to every other risk.
Today’s Topics

- Malware
- Identity theft
- Account hacking
- Scams and frauds
- Cyberbullying
Malware - “Malicious software”

• Definition: Software that gets installed on your computer without your consent.
• Types: Viruses, spyware, bots, adware, Trojan horses.
• Potential damage: cause your computer to crash or work very slowly, pass on viruses to other computers, strangers can monitor your activity.
• How to detect malware: slow computer, computer won’t shut down or restart, pop-up ads, browser opens web pages you didn’t choose.
Protect yourself from malware

**DO NOT**

- Click on links in emails (even those that appear to be from friends).
- Open attachments in emails (even those that appear to be from friends).
- Click on pop-ups that appear - no matter how interesting they appear to be.

**DO**

- Keep your operating system up-to-date.
- Keep your internet security software up-to-date and activated (it regularly scans your computer).
- Be aware of what is ‘normal’ for your computer - how fast it runs, how websites look.
You’ve got Malware! Now what?

- If you have active anti-virus software on your computer, that software did NOT spot and stop the malware. Make sure your software is up-to-date.


- Microsoft offers a free on-demand malware scanner that works with your existing antivirus software - https://www.microsoft.com/security/scanner/en-us/Fr
Today’s Topics

• Malware
• Identity theft
• Account hacking
• Scams and frauds
• Cyberbullying
Identity Theft

• Definition: crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

• Potential damage: applying for loans in your name (affecting your credit history), withdrawing funds from banking accounts, filing tax returns in your name.

• How to detect identity theft: unexplained change in credit score, official mail from bona fide organizations (IRS, bank, retailer) about possible exposure, official mail from bona fide organizations about a transaction you did not make.
Techniques

- Paying petty thieves for stolen wallets.
- Dumpster-diving.
- Shoulder-surfing.
- Account hacking.
- Phishing.
Phishing

• An email or phone call purporting to be from a company.
• Attempt to get you to enter or provide account or other personal information.
• NO legitimate company will send you an email asking you for your username and password.
• NO legitimate company will call you and ask you for your information.
• To be safe, call the company yourself or go directly to the website on your computer.
Phishing example

Subject: Important information!

Dear HSBC Customer,

Your Internet Banking security number was entered incorrectly more than 3 times. For the protection of your account we have suspended access to it. To restore access please Log on correctly.

Previous notifications have been sent.

Thank you for choosing HSBC Bank. 
Copyright HSBC INC 2010. All rights reserved.
Phishing characteristics

• Bad spelling or grammar.
• Incorrect information.
• Sender email address does not match purported website (e.g., amazon.org, amazon-security.com).
• Sense of urgency.
• Often refers to internet security or invoices, orders, or payments.
Check your Spam folder

Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)

- Derick Curry
  Payment Confirmation - Dear Valued Customer, Your invoice appears below. Please remit payment at your earliest convenience.
  Mar 2

- Weldon pardue
  Unpaid invoice # 00239167 - Dear Client, According to the reconciliation of the Department of Finance there are the arrears
  Mar 1

- Penny batu
  Invoice #3295558/15 - Dear costumer, You are receiving this informational letter because of the fact that you have a debt
  Feb 29

- Facebook
  You have more friends on Facebook than you think - The fastest way to find all of your friends on Facebook is importing your email contacts. Once you
  Feb 29

- Facebook
  You have more friends on Facebook than you think - The fastest way to find all of your friends on Facebook is importing your email contacts. Once you
  Feb 25

- Bertha Garcia
  Invoice 85413452 - Dear akaga. Please review the attached copy of your Invoice (number: IN85413452) for an amount of
  Feb 24

- Matt Alleman
  Central phones - The phones at central are having issues calling out. It should be fixed soon but I apologize for the
  Feb 23
Protect yourself from identity theft

- Do not give any personal or account information in a telephone call you did not initiate or when prompted by an email you received.
- Be aware of your surroundings any time you give information over the telephone or on a computer (“shoulder surfing”).
- Shred documents with personal information.
- Do not carry your Social Security card in your wallet. Only give your SSN when you absolutely have to.
- Retrieve your USPS mail frequently.
- Monitor your bank and credit card statements. Be aware of your billing cycles.
Today’s Topics

• Malware - including viruses, spyware
• Identity theft
• Account hacking
• Scams and frauds
• Cyberbullying
Account hacking

• Definition: Somebody accesses your account without your permission.
• Types: Email, social media, websites.
• Potential damage: identity theft, professional or personal reputation.
• How to detect hacking: your account username and password don’t work, you are locked out of your account, your friends tell you they received a strange email from you, your Facebook timeline includes something you didn’t post.
Ways you can get hacked

• Brute force: someone has your email address and guesses at the password.

• Man-in-the-middle: you are on a public wi-fi network or on an unencrypted home wi-fi network and not using an encrypted site.

• Trojan horse: you have downloaded and installed software that gives hackers access to your keystrokes.

• Phishing: you log in to or provide your account information to a look-alike website or company communication.
What to do if your account is hacked

• Notify all of your contacts that they may receive spam messages that appear to come from you - warn them not to open messages or click on any links from your account.

• If you believe your computer is infected, be sure your security software is up to date and scan your system for malware.

• Change passwords on all accounts that have been hacked ASAP.

• If you cannot access your account because a password has been changed, contact the website immediately and follow any steps they have for recovering an account.
Strong passwords

• Use a combination of lower-case and upper-case letters, numbers, and special characters (e.g., /, @, #).

• For your own benefit, devise a password that is easy for you to remember (but hard for others to figure out).

• Substitute numbers for letters.

• Substitute special characters for letters.

• At least 8 characters long.

• Do NOT use street address, pets’ names, children’s names, birthdates, or similar information.
You have a secure connection if...

<table>
<thead>
<tr>
<th>Browser</th>
<th>Secure Indicator</th>
<th>Example Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Green padlock image to the left of the website name</td>
<td><img src="https://www.wellsfargo.com" alt="https://www.wellsfargo.com" /></td>
</tr>
<tr>
<td></td>
<td>and website name begins with <code>https://</code></td>
<td></td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Green padlock image to the left of the website name</td>
<td><img src="https://ssa.gov" alt="Social Security Administration (US)" /></td>
</tr>
<tr>
<td></td>
<td>and website name begins with <code>https://</code></td>
<td></td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Padlock image to the right side of the website name</td>
<td><img src="https://twitter.com/" alt="Twitter" /></td>
</tr>
<tr>
<td></td>
<td>and website name begins with <code>https://</code></td>
<td></td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Padlock image to the left of the website name</td>
<td><img src="https://facebook.com" alt="Facebook" /></td>
</tr>
</tbody>
</table>
A secure connection ...

• ...means that your information is encrypted and sent to the recipient, then decrypted at the recipient’s end. Information sent to you by the recipient is decrypted, then sent, and decrypted for your use.

• ...does NOT mean that you are connected to a legitimate business or organization. For example, if you click on a link in a phishing email that looks like an Amazon email, you may find yourself in a website with a secure connection, but it will not necessarily be the Amazon website.
Wireless and public connections

• Use encryption and password protection options on wireless router in home network
• Be wary of accessing sensitive information when using public wi-fi networks. Make sure encryption is on (https).
• Be aware of how you log in to any accounts when on a public computer - don’t turn on option to “keep me signed in”. Make sure to always log off.
Today’s Topics

• Malware - including viruses, spyware
• Identity theft
• Account hacking
• Scams and frauds
• Cyberbullying
Scams and frauds

• Definition: dishonest way to make money by deceiving people (scam, Merriam-Webster) via the internet.
• Types: Nigerian (419), traveler in distress, sweepstakes winner.
• Potential damage: financial loss.
• How to detect scams and frauds: too good to be true, sense of urgency, requests for account numbers or personal information, requires cash up-front.
• https://www.fbi.gov/scams-safety/fraud/internet_fraud
Today’s Topics

• Malware - including viruses, spyware
• Identity theft
• Account hacking
• Scams and frauds
• Cyberbullying
Cyberbullying

• Definition: act of harming or harassing using information technology networks in a repeated and deliberate manner

• Examples:
  • Sending mean or threatening emails, instant messages, or text messages
  • Tricking someone into revealing personal or embarrassing information and sending it to others
  • Breaking into someone’s email or instant message account to send cruel or untrue messages while posing as that person
  • Creating websites to make fun of another person (e.g. classmate)

• [http://www.ncpc.org/topics/cyberbullying/stop-cyberbullying](http://www.ncpc.org/topics/cyberbullying/stop-cyberbullying)
Resources for parents of children

- [http://www.gcflearnfree.org/internetsafetyforkids](http://www.gcflearnfree.org/internetsafetyforkids) (GCFFreeOnline)
- [https://www.onguardonline.gov/topics/protect-kids-online](https://www.onguardonline.gov/topics/protect-kids-online) (OnGuardOnline.gov is a unit of the Department of Homeland Security)
- [http://www.gcflearnfree.org/internetsafetyforkids/3](http://www.gcflearnfree.org/internetsafetyforkids/3) (cyberbullying from GCFFreeOnline)
Resources for parents of teens

- [https://support.google.com/youtube/answer/2802244](https://support.google.com/youtube/answer/2802244) (YouTube’s safety information for parents)
- [https://www.facebook.com/safety/groups/parents/](https://www.facebook.com/safety/groups/parents/) (Facebook’s information for parents)
Internet Safety

QUIZ!
You can safely enter personal information into a website if...

• You entered the URL (website name) yourself.
• You recognize the company name and logo on the home page.
• You followed a link from a website you know and trust.
• There is a green padlock image to the left of the website name and the website name begins with https://
Criminals need one or more of the following to steal your identity...

• Social security number.
• Mailing address.
• Date of birth.
• Email address.
• Mother’s maiden name.
• Place of birth.
Which of these is a symptom that your email account has been hacked?

• You receive email advertisements from a company you don’t recognize.
• You can’t log into your email account.
• Your internet connection at home stops working.
• Friends tell you they emailed you something, but you haven’t received it.
• You can’t find an old email message.
• Friends tell you they received an odd email message from you.
Which of these is the strongest password?

- Daisy59
- rfvujm
- Gren@Dier/7
- Broncosfan
Which of these are examples of identity theft?

• Someone files a federal tax return using your social security number.
• Someone applies for a loan using your name and date of birth.
• Someone uses your credit card without your permission.
• Someone opens up a bank account with your name and address.
• Someone cashes a check made out to you.
• Someone creates an email account with your first and last name.
Which of these are examples of malware?

• Virus
• Trojan horse
• Roman chariot
• Adware
• Hacking
• Software
• Spyware
Internet safety research guide

• Library website - www.mesacountylibraries.org
• eResources
• Research guides
• Internet safety